UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/954,976	09/18/2001	Surendra N. Naidoo	4017-03001	8803

30652 7590 03/17/2008
CONLEY ROSE, P.C.
5601 GRANITE PARKWAY, SUITE 750
PLANO, TX 75024

EXAMINER	
VO, TUNG T	
ART UNIT	PAPER NUMBER
2621	
MAIL DATE	DELIVERY MODE
03/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/954,976	**Applicant(s)** NAIDOO ET AL.	
	Examiner Tung Vo	**Art Unit** 2621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-24,26-31 and 47-61* is/are pending in the application.

4a) Of the above claim(s) *2,25 and 32-46* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-24,26-31 and 47-61* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10/26/07; 10/31/03*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/26/2007 has been entered.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-19, 47-49, and 53-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsumpes (US 6,442,241 B1).

Re claim 1, Tsumpes discloses a security system (fig. 1) comprising:

a security gateway located at a premises (11 and 12 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video (Alarm inputs, 11 of fig. 1, wherein alarm inputs 11 are video, so this would obviously be considered as alarm video; col. 8, lines 45-50, note the digital data packet DDP and wireless or

Internet communication network also enables the present system to provide video and/or audio transmissions from the monitored device or premises to the central monitoring station due to the bandwidth capabilities of most digital data packet networks);

a security system server (13 of fig. 1) operatively coupled to the security gateway through a first network (PSTN of fig. 1), wherein the security gateway is configured to notify the security system server of the alarm condition (col. 6, lines 32-58) and to transfer the Alarm Video to the security system server in substantially real time through the first network (col. 4, line 64-col. 5, line 33, alternative transmission of notification alarms between the security gateway and the security system server, 12 and 13 of fig. 1);

wherein the security system server (13 of fig. 1) is further operatively coupled to the security gateway (12 of fig. 1) through a second network (CELLULAR BASE STATION or WIRELESS of fig. 1, wherein WIRELESS is considered a second network),

wherein the security gateway (12 of fig. 1) is configured to notify the security system server of the alarm condition through the second network (WIRELESS of fig. 1),

wherein the security gateway (12 of fig. 1) is further configured to notify the security system server of the alarm condition through the first network (PSTN of fig. 1) substantially simultaneously with notifying the security system server of the alarm condition through the second network (note the subscriber may also instruct the system (10 of fig. 1) to simultaneously notify them at the subscriber's work number, home number, cell phone number, pages number, and to send a fax, and/or email message, upon the occurrence of a particular event; this disclosure fairly suggest the PSTN of fig. 1 used for the first network and simultaneously the WIRELESS of fig. 1 used for second network), and wherein the security system server thereby receives two notifications of the alarm condition from the security gateway (the security system server as central monitoring station receives one or more alarms from the premises, col. 1, lines 15-25).

Re claims 3-12, Tsumpes further teaches the first network is an IP network, an Ethernet-based network, Internet, a frame relay network, a hybrid-fiber coaxial network, a fiber-optic network, a DSL network, an ATM network, a high-speed fixed wireless network, a high-speed mobile communications network (DDP, DMTF, WIRELESS of fig. 1; One skill in the art would use the well known and suitable network that are available in the market).

Re claim 13, Tsumpes further teaches the second network comprises a public switched telephone network, a fixed wireless network, a mobile communications network (DDP of fig. 1).

Re claim 16, Tsumpes further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred to hereinafter as Alarm Audio, and wherein the security gateway is further configured to transmit said Alarm Audio to the security system server through the second network in substantially real time (col. 8, lines 45-50).

Re claims 17 and 18, Tsumpes further teaches wherein the security system server is configured to provide notification of the alarm condition to a public safety agency (user or further security services fig. 1).

Re claim 19, Tsumpes further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred to hereinafter as Alarm Audio, and wherein the security gateway is further configured to transmit said Alarm Audio to the security system server through the first network in substantially real time (col. 8, lines 45-50).

Re claims 53-56, Tsumpes further teaches a security system comprising (fig. 1): a security gateway located at a premises (11 and 12 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video; and

a security system server (13 of fig. 1) operatively coupled to the security gateway through a first network (PSTN of fig. 1), wherein the security gateway is configured to notify the security system server of the alarm condition and to transfer the Alarm Video to the security system server through the first network in substantially real time;

wherein the security system server is further operatively coupled to the security gateway through a second network (WIRELESS of fig. 1),

wherein the security gateway is configured to: (1) notify the security system server of the alarm condition through the second network (WIRELESS of fig. 1); (2) detect if connectivity with the security system server through the first network is lost (col. 3, lines 54-63); and (3) notify the security system server through the second network of the loss of connectivity through the first network (Back-up communications channel).

wherein the security gateway (12 of fig. 1) is further configured to: (4) notify the security system server in the event that connectivity with the security system server through the first network is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored.

4. Claims 1, 3-19, 47-49, and 53-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lemons (US 6,504,479) in view of Tsumpes (US 6,442,241 B1).

Re claim 1, Lemons discloses a security system (10 of fig. 1) comprising: a security gateway (12, 14 of fig. 1) located at a premises (figs. 5-8), wherein the security gateway (12 of fig. 1) is operable to detect an alarm condition (18 of fig1; col. 6, lines 42-51) and to record video (20 of figs. 1 and 2) of at least a portion of the premises relating to the alarm condition, said video hereafter referred to as an alarm video (col. 7, lines 25-50); and a security system server (38 of fig. 1) operatively coupled to the security gateway through a first network (36 of fig. 1), wherein the security gateway is configured to notify the security system server of the alarm condition and to transfer the alarm video to the security system server in substantially real time through the first network (col. 7, lines 25-28); wherein the security system server (12, 14 of fig. 1) is further operatively coupled to the security gateway through a second network (50 of fig. 1); wherein the security gateway is configured to notify the security system server of the alarm through the second network (col. 4, line 66-col. 5, line 30), and wherein the security gateway (12 of fig. 1) is further configured to notify the security system server (38 of fig. 1) of the alarm condition through the first network (26 of fig. 1) substantially with notify the security system server (38 of fig. 1) of the alarm condition through the second network (50 of fig. 1) if the first network is lost.

Lemons suggests that any communications channel available (36 and 50 of fig. 1) to connect between the gateway (12 of fig. 1) and the security server would be used for backup (if the network 36 is down, so network (50) is used for backup) or redundant (usable the same in communications), so this is evidence to one skilled in the art to modify any conventional network into the security system of Lemons.

However, Lemons does not particularly teach the notification of alarm video transmits to the first and second networks simultaneously and the security system server thereby receives two notifications of the alarm condition from the circuitry gateway as claimed.

Tsumpes teaches the notification of alarm video transmits to the first and second networks simultaneously (DTMF, DDP, and CELLULAR BASE STATION (WIRELESS) of fig. 1, automated parallel and redundant contact, cols. 3-4; note the system enables automated simultaneous contact of one or more persons over a plurality of telephonic and electronic communication channels and provides parallel event-specific notification via voice, pager, voice mail, fax and email to the recipient(s)) and the security system server (13 of fig. 1) thereby receives two notifications of the alarm condition from the circuitry gateway (11 and 12 of fig. 1, note this invention relates generally to alarm and event notification methods and systems, and more particularly to an automated parallel and redundant subscriber contact and event notification system and method that enables automated simultaneous contact and notification of one or more authorized persons over a plurality of telephonic and electronic communications channels including wireless, voice, pager, voice mail, fax and email to provide specific event information relative to one or more monitored (inputs), sensors or alarms)

Therefore, taking the teachings of Lemons and Tsumpes as a whole, it would have been obvious to one of ordinary skill in the art to modify the teachings of Tsumpes, the automated parallel and redundant contact to a user notification one or more alarms, into the security system of Lemons for one of the major benefits of the automated parallel and redundant contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations.

Re claims 3-12, Lemons further teaches wherein the first network is an IP network (a network in which transmission of information is done using IP protocol; e.g. Internet network), an Ethernet-based network (LAN), the Internet, a frame relay network (a frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN); a DSL network; a high-speed fixed wireless network (36 of fig. 1; see col. 5, lines 18-23); Lemons further suggests any communications channel available (36 and 50 of fig. 1) such as a hybrid-fiber coaxial network; a fiber-optic network, an ATM network, and a high-speed mobile communications network, that connects between the gateway (12 of fig. 1) is used in the security system.

Re claims 13-15, Lemons further teaches wherein the second network comprises a public switched telephone network and a fixed wireless network (col. 5, lines 25-30).

Re claims 16 and 19, Lemons further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred to hereinafter as alarm audio, alarm video, and wherein the security gateway is further configured to transmit said alarm audio and video to the security system server through the second network in substantially real time (102, 108, 110, 112, 114, 116, and 118 of fig. 2; alarm 144 and 160 of fig. 3).

Re claims 17 and 18, Lemons further teaches wherein the security system server is configured to provide notification of the alarm condition to a public safety agency (42, 44, 46, and 48 of fig. 1).

Re claims 47-49 and 53-56, Lemons teaches a security system (10 of fig. 1) comprising: a security gateway (12 of fig. 1) located at a premises, wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video; and a security system server (38 of fig. 1) operatively coupled to the security gateway through a first network (36 of fig. 1), wherein the security gateway is configured to notify the security system server of the alarm condition and to transfer the Alarm Video to the security system server through the first network in substantially real time; wherein the security system server (38 of fig. 1) is further operatively coupled to the security gateway through a second network (50 of fig. 1), wherein the security gateway is configured to: (1) notify the security system server of the alarm condition through the second network (50 of fig. 1); (2) detect if connectivity with the security system server through the first network is lost (col. 4, line 66-col. 5, line16; note the communications channel (50) is used for redundant or backup; when the communications channel (36) is down or lost, the communications channel (50) is used for transmitting the notification, this disclosure suggest that the connectivity would obviously detected); and (3) notify the security system server (38 of fig. 1) through the second network (50 of fig. 1) of the loss of connectivity through the first network (36 of fig. 1, Note if the first network fails); wherein the security gateway (12 of fig. 1) is further configured to: (4) notify the security system server in the event that connectivity with the security system server through the first network (36 of fig. 1) is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored (col. 5, lines 1-16).

5. Claims 57-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lemons (US 6,504,479) in view of Menard (US 6,667,688).

Re claims 57-61, Lemons teaches a security system (fig. 1) comprising: a security gateway located at a premises (12 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, the video hereinafter referred to as an Alarm Video (16, 18, 20, 22, and 14 of fig. 1); a security system server (38 of fig. 1) operatively coupled to the security gateway (12 of fig. 1) through a first network (36 of fig. 1), wherein the security gateway is configured to notify the security system server of the alarm condition and to transfer the Alarm Video to the security system server through the first network in substantially real time and wherein the security system server is remotely located relative to the security gateway (160 of fig. 3);

It is noted that Lemons teaches the monitor center (48 of fig. 1) for monitoring video images, display alarms, display of contact data and information, wherein the video image and alarms received through network (36 or 50 of fig. 1), and any conventional channel communication networks include standard telephone service, ISDN, DSL, Internet, dedicated cable, local area network, wide area network, wireless, or any communications channel available to connect between the promise and server or other (col. 5, lines 15-22).

However, Lemons does not particularly teach a monitoring center operatively coupled to said security gateway through a second network, wherein the security gateway is configured to notify the monitoring center of the alarm condition through the second network, wherein the monitoring center is remotely located relative to the security gateway and the security system server and wherein the monitoring center is further operably coupled to the security system server; and wherein the monitoring center is configured to notify the security system server of the alarm condition; wherein the monitoring center is operatively coupled to the security system server through a third network and wherein the monitoring center is configured to notify the security system server of the alarm condition through the third network; wherein the security system gateway is configured to notify the security gateway of the alarm condition through the first network substantially simultaneously with notifying the monitoring station of the alarm condition through the second network; wherein the monitoring center is operatively coupled to the security system server through the first network and wherein the monitoring center is configured to notify the security system server of the alarm condition through the first network; wherein the security system gateway is configured to notify the security gateway of the alarm condition through the first network substantially simultaneously with notifying the monitoring station of the alarm condition through the second network as specified in claims 57-61.

Menard teaches a monitoring center (30 and 40 of fig. 1, Note user communication device is considered as monitoring center) operatively coupled to said security gateway (10 of fig. 1) through a second network (Path A of fig. 1), wherein the security gateway (10 of fig. 1) is configured to notify the monitoring center of the alarm condition through the second network (alarm transmission of fig. 1), wherein the monitoring center (30 and 40 of fig. 1) is remotely located relative to the security gateway (10 of fig. 1) and the security system server (20 of fig. 1) and wherein the monitoring center is further operably coupled to the security system server (30, 40, and 20 of fig. 1); and wherein the monitoring center is configured to notify the security system server of the alarm condition (Path D carries the same alarm transmission as Path A of fig. 1); wherein the monitoring center (30 and 40 of fig. 1) is operatively coupled to the security system server through a third network (Path D of fig. 1) and wherein the monitoring center (30 of fig. 1) is configured to notify the security system server of the alarm condition through the third network (Path C of fig. 1); wherein the security system gateway (10 of fig. 1) is configured to notify the security gateway of the alarm condition through the first network substantially simultaneously with notifying the monitoring station of the alarm condition through the second network (Path A and Path B of fig. 1, Note simultaneous alarm transmission); wherein the monitoring center (30 and 40 of fig. 1) is operatively coupled to the security system server (Path D is the same Path A of fig. 1) through the first network and wherein the monitoring center is configured to notify the security system server of the alarm condition through the first network (Path A as Path D); wherein the security system gateway (10 of fig. 1) is configured to notify the security gateway (Alarm system) of the alarm condition through the first network substantially simultaneously with notifying the monitoring station of the alarm condition through the second network (Path A of fig. 1).

Therefore, taking the teachings of Lemons and Menard as a whole, it would have been obvious to one of ordinary skill in the art to modify the first and second networks (Path A and Path B of fig. 1) of Menard into the security system of Lemons for automatically transmitting notification of a detected alarm to the user. Doing so would save cost and simplify the security system.

6. Claims 20-24, 26-31, and 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lemons (US 6,504,479) in view of Tsumpes (US 6,442,241 B1) and further in view of Kung et al. (US 6,826,173).

Re claim 20, Lemons teaches a security system (fig. 1) comprising: a security gateway (12 of fig. 1) located at a premises (12a and 12b of fig. 8), wherein the security gateway (12 of fig. 1) is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition to form an alarm video (16, 18, 20, 22 of fig. 1; see fig. 3), wherein the security gateway (12 of fig. 1) further comprises a network interface (14 of fig. 1, Note the connections between the components (24, 26, 28, 30, 34, 56 of fig. 1), and wherein the network interface is configured to connect the security gateway a head-end through out a first network (col. 6, line 62-col. 7, lines 50, Note the connections between components are considered as the first network; a network is a fabric or structure of cords or wires that cross at regular intervals and are knotted or secured at the crossings, a system of lines or channels resembling a network, an interconnected or interrelated chain, group, or system, or a system of computers, peripherals, terminals, and databases connected by communications lines); a security system server (38 of fig. 1) configured to connect to the interface (34 of fig. 1) through a second network (36 of fig. 1), wherein the security gateway (12 and 14 of fig. 1) is configured to notify the security system server of the alarm condition and to transfer the alarm Video to the security system server in substantially real time (col. 7, lines25-50); wherein the security gateway (12, 14 of fig. 1) is operatively coupled to the security system server (38 of fig. 1) through a third network (50 of fig. 1), the security gateway being further configured to notify the security system server of the alarm condition through the third network (col. 4, line 66 through col. 5, lines 14);

and However, Lemons suggests that any communications channel available (36 and 50 of fig. 1) such as a hybrid-fiber coaxial network; a fiber-optic network, an ATM network, and a high-speed mobile communications network, that connects between the gateway (12 of fig. 1) is used in the security system, so this is evidence to one skilled in the art to modify any conventional network into the security system of Lemons.

It is noted that Lemons does not particularly teach simultaneously notifying the alarm to the security server of the alarm through the second network and the third network, and wherein the security system server is configured to receive a notification of the alarm condition through the second network and to receive another notification of the alarm condition through the third network as claimed.

Tsumpes teaches simultaneously notifying the alarm to the security server (113) of the alarm through the second network (PSTN of fig. 1) and the third network (CELLULAR BASE STATION of fig. 1, WIRELESS), and wherein the security system server (13 of fig. 1) is configured to receive a notification of the alarm condition through the second network (PSTN of fig. 1) and to receive another notification of the alarm condition through the third network (WIRELESS of fig. 1; note one or more alarms can be received at the central station, 13 of fig. 1; the disclosure of Tsumpes relates generally to alarm and event notification methods and systems, and more particularly to an automated parallel and redundant subscriber contact and event notification system and method that enables automated simultaneous contact and notification of one or more authorized persons over a plurality of telephonic and electronic communications channels including wireless, voice, pager, voice mail, fax and email to provide specific event information relative to one or more monitored (inputs), sensors or alarms)

Therefore, taking the teachings of Lemons and Tsumpes as a whole, it would have been obvious to one of ordinary skill in the art to modify the teachings of Tsumpes, the automated parallel and redundant contact to a user notification one or more alarms, into the security system of Lemons for one of the major benefits of the automated parallel and redundant contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations.

The combination of Lemons and Tsumpes teaches all limitation above, except the interface of the security gateway connects to a cable head-end through the first network by a hybrid-fiber-coaxial network as claimed.

However, Kung teaches a security gateway (102 of fig. 1) connects to a cable head-end (115 of fig. 1) through a first network (112 of fig. 1) by a hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9).

Therefore, taking the teachings of Lemons, Tsumpes, and Kung as a whole, it would have been obvious to one of ordinary skill in the art to incorporate the cable head-end (115 of fig. 1) through the first network (112 of fig. 1) by the hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9) of Kung into the communications channel (34 and 36 of fig. 1) of the combined security of Lemons and Tsumpes for the same purpose of transmitting the alarm video and alarm condition from the security gateway to the security server. Doing so would provide improved performance and quicker response time for an individual user.

Re claims 21-24, 26-28, Lemons further teaches the first network is an IP network (a network in which transmission of information is done using IP protocol; e.g. Internet network), an Ethernet-based network (LAN), the Internet, a frame relay network (a frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANS) and between end-points in a wide area network (WAN); a DSL network; a high-speed fixed wireless network (36 of fig. 1; see col. 5, lines 18-23); Lemons further suggests any communications channel available (36 and 50 of fig. 1) such as a hybrid-fiber coaxial network; a fiber-optic network, an ATM network, and a high-speed mobile communications network, that connects between the gateway (12 of fig. 1) is used in the security system; and wherein the second network comprises a public switched telephone network and a fixed wireless network (col. 5, lines 25-30).

Re claim 29, Lemons further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred to hereinafter as alarm audio, alarm video, and wherein the security gateway is further configured to transmit said alarm audio and video to the security system server through the second network in substantially real time (102, 108, 110, 112, 114, 116, and 118 of fig. 2; alarm 144 and 160 of fig. 3).

Re claims 30 and 31, Lemons further teaches wherein the security system server is configured to provide notification of the alarm condition to a public safety agency (42, 44, 46, and 48 of fig. 1).

Re claims 50-52, Lemons further teaches a security system (10 of fig. 1) comprising: a security gateway (12 of fig. 1) located at a premises, wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video; and a security system server (38 of fig. 1) operatively coupled to the security gateway through a first network (36 of fig. 1), wherein the security gateway is configured to notify the security system server of the alarm condition and to transfer the Alarm Video to the security system server through the first network in substantially real time; wherein the security system server (38 of fig. 1) is further operatively coupled to the security gateway through a second network (50 of fig. 1), wherein the security gateway is configured to: (1) notify the security system server of the alarm condition through the second network (50 of fig. 1); (2) detect if connectivity with the security system server through the first network is lost (col. 4, line 66-col. 5, line16); and (3) notify the security system server (38 of fig. 1) through the second network (50 of fig. 1) of the loss of connectivity through the first network (36 of fig. 1, Note if the first network fails); wherein the security gateway (12 of fig. 1) is further configured to: (4) notify the security system server in the event that connectivity with the security system server through the first network (36 of fig. 1) is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored (col. 5, lines 1-16).

7. Claims 20-24 and 26-31, 47-52, 55-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saylor (US 6,400,265) in view of Kung et al. (US 6,826,173), and further in view of Tsumpes (US 6,442,241 B1).

Re claim 20, Saylor teach a security system (fig. 1) comprising: a security gateway located at premises (110, 120, 112, 122, 114, and 124 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video (120, 122, and 124 of fig. 1), wherein the security gateway further comprises a network interface (100 of fig. 1, wherein the connections between the property (110 of fig. 1) and a security server (130 of fig. 1) throughout the network (100 of fig. 1)), and wherein the network interface is configured to connect the security gateway to a cable head-end through a first network (Note the network (100 of fig. 1) between the property (110 of fig. 1) and the security server (130 of fig. 1); a security system server (130 of fig. 1) configured to connect to the cable head-end through a second network (150 of fig. 1, Note alert notification is sent to the user and to the security system server through out the Internet), wherein the security gateway (110 of fig. 1) is configured to notify the security system server (130 of fig. 1) of the alarm condition and to transfer the Alarm Video to the security system server in substantially real time through the second network (col. 4, lines 44-47); wherein the security gateway (110 of fig. 1) is operatively coupled to the security system server (130 of fig. 1) through a third network (152 of fig. 1; Note alert notification is transmitted to the user and to the security system server through POTS (cable)), the security gateway (110 of fig. 1) being further configured to notify the security system server (130 of fig. 1) of the alarm condition through the third network (152 of fig. 1); and wherein the security gateway (110 of fig. 1) is configured to notify the security system server of the alarm condition through the second network substantially simultaneously (Note a system and method for monitoring a security system by using video images where a wireless communication system may be used to automatically inform an owner and other authorized entities in a manner predetermined by the user when alarm situations and/or alarm worthy situations occur, this suggests the security gateway simultaneously transmits the alarm notification to the second and third networks)with notifying the security system server (130 of fig. 1) of the alarm condition through the second and third networks (150 and 152 of fig. 1).

It is noted that Saylor suggests that phone, POTS, cable, DSL, and other combinations may be implemented (col. 6, lines 21-33), so this is evidence to one skill in the art to modify any conventional and suitable connector(s) between the security server and the security gateway of Saylor. However, Saylor does particularly teach the first network is a hybrid-fiber- coaxial network as claimed.

Kung teaches a security gateway (102 of fig. 1) connects to a cable head-end (115 of fig. 1) through a first network (112 of fig. 1) by a hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9).

Therefore, taking the teachings of Saylor and Kung as a whole, it would have been obvious to one of ordinary skill in the art to incorporate the cable head-end (115 of fig. 1) through the first network (112 of fig. 1) by the hybrid-fiber-coaxial network (col.5, line 44 through col. 6, line 9) of Kung into the networks of Saylor for enhancing the functionality of components in the broadband network. Doing so would allow the system to provide ease of maintenance, control, and re-configuration as well as a reduction in cost due to shared functionality.

It is noted that Saylor does not particularly wherein the security system server is configured to receive a notification of the alarm condition through the second network and to receive another notification of the alarm condition through the third network as claimed.

Tsumpes teaches simultaneously notifying the alarm to the security server (13) of the alarm through the second network (PSTN of fig. 1) and the third network (CELLULAR BASE STATION of fig. 1, WIRELESS), and wherein the security system server (13 of fig. 1) is configured to receive a notification of the alarm condition through the second network (PSTN of fig. 1) and to receive another notification of the alarm condition through the third network (WIRELESS of fig. 1; note one or more alarms can be received at the central station, 13 of fig. 1; the disclosure of Tsumpes relates generally to alarm and event notification methods and systems, and more particularly to an automated parallel and redundant subscriber contact and event notification system and method that enables automated simultaneous contact and notification of one or more authorized persons over a plurality of telephonic and electronic communications channels including wireless, voice, pager, voice mail, fax and email to provide specific event information relative to one or more monitored (inputs), sensors or alarms)

Therefore, taking the teachings of Saylor, Kung, and Tsumpes as a whole, it would have been obvious to one of ordinary skill in the art to modify the teachings of Tsumpes, the automated parallel and redundant contact to a user notification one or more alarms, into the security system of Saylor and Kung for one of the major benefits of the automated parallel and redundant contact and notification system and method is that it provides expeditious and efficient handling of time sensitive events and significantly reduces response time in emergency situations.

Re claim 21, Saylor teaches wherein the second network is a dedicated bandwidth network (Internet 150 of fig. 1).

Re claim 22, Saylor further teaches wherein the second network comprises a frame relay network (230 of fig. 1).

Re claim 23, Saylor further teaches wherein the second network comprises an ATM network (other methods are considered as an ATM network, col. 4, lines 46-47).

Re claim 24, Saylor further teaches wherein the second network comprises a managed IP connection having quality of service (TCP/IP connection of fig. 2).

Re claim 26, Saylor further teaches wherein the third network comprises a public switched telephone network (POTS 152 of fig. 1).

Re claim 27, Saylor further teaches wherein the third network comprises a fixed wireless network (fig. 2).

Re claim 28, Saylor further teaches wherein the third network comprises a mobile communications network (col. 4, line 46).

Re claim 29, Saylor further teaches wherein the security gateway is further operable to record audio from at least a portion of the premises relating to the alarm condition, said audio referred hereinafter as Alarm Audio, and wherein the security gateway is further configured to transmit said Alarm Audio to the security system server through the second network in substantially real time (col. 8, lines 50-65).

Re claim 30, Saylor further teaches wherein the security system server (130 of fig. 1) is configured to provide notification of the alarm condition to a public safety agency (160f-160N of fig. 1; see also 164 of fig. 1).

Re claim 31, Saylor further teaches wherein the security system server is further configured to provide the Alarm Video to the public safety agency (video 110 of fig. 1).

Re claim 47, Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and notify the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 50-55).

Re claim 48, Saylor further teaches wherein the security gateway is further configured to notify the security system server in the event that connectivity with the security system server through the first network is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored (col. 6, lines 21-34).

Re claim 49, Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and notify the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 21-34).

Re claim 50, Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and notify the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 21-34).

Re claim 51, Saylor further teaches wherein the security gateway is further configured to notify the security system server in the event that connectivity with the security system server through the first network is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored (col. 6, lines 21-55).

Re claim 52, Saylor further teaches wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and notify the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 21-55).

Re claim 55, Saylor further teaches a security system (fig. 1) comprising: a security gateway located at a premises (110, 120, 112, 122, 114, and 124 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, said video hereinafter referred to as an Alarm Video (120, 122, and 124 of fig. 1); and a security system server (130 of fig. 1) operatively coupled to the security gateway through a first network, wherein the security gateway is configured to notify the security system server of the alarm condition and to transfer the Alarm Video to the security system server in substantially real time through the first network (100 of fig. 1, Note the connections between the property and the central security would obviously be considered as a first network); wherein the security system server (130 of fig. 1) is further operatively coupled to the security gateway through a second network (150 of fig. 1), wherein the security gateway is configured to notify the security system server of the alarm condition through the second network; and wherein the security gateway is further configured to notify the security system server in the event that connectivity with the security system server through the first network is lost while the security gateway is disarmed and the security gateway is armed before connectivity with the security system server through the first network is restored (col. 6, lines 21-55).

Re claim 56, Saylor further discloses wherein the security gateway is further configured to detect if connectivity with the security system server through the first network is lost and notify the security system server through the second network of the loss of connectivity through the first network (col. 6, lines 21-55).

Re claim 57, Saylor further teaches a security system (fig. 1) comprising: a security gateway located at a premises (110, 120, 112, 122, 114, 124 of fig. 1), wherein the security gateway is operable to detect an alarm condition and to record video of at least a portion of the premises relating to the alarm condition, the video hereinafter referred to as an Alarm Video; a security system server (130 of fig. 1) operatively coupled to the security gateway through a first network, wherein the security gateway is configured to notify the security system server of the alarm condition and to transfer the Alarm Video to the security system server through the first network in substantially real time and wherein the security system server is remotely located relative to the security gateway (Note the connections between the security server and the property would obviously be considered as a first network, see 110, 130 of fig. 1)); a monitoring center (160 of fig. 1) operatively coupled to said security gateway through a second network (150 of fig. 1), wherein the security gateway is configured to notify the monitoring center of the alarm condition through the second network, wherein the monitoring center (160 of fig. 1) is remotely located relative to the security gateway and the security system server and wherein the monitoring center is further operably coupled to the security system server (130 of fig. 1); and wherein the monitoring center is configured to notify the security system server of the alarm condition (160 of fig. 1).

Re claim 58, Saylor further discloses wherein the monitoring center is operatively coupled to the security system server (130 of fig. 1) through a third network (152 of fig. 1) and wherein the monitoring center is configured to notify the security system server of the alarm condition through the third network.

Re claim 59, Saylor further teaches wherein the security system gateway is configured to notify the security gateway of the alarm condition through the first network substantially simultaneously with notifying the monitoring station of the alarm condition through the second network (col. 1, lines 5-13).

Re claim 60, Saylor further teaches wherein the monitoring center (160 of fig. 1) is operatively coupled to the security system server (130 of fig. 1) through the first network (Internet) and wherein the monitoring center is configured to notify the security system server of the alarm condition through the first network.

Re claim 61, Saylor further teaches wherein the security system gateway (110 and 120 of fig. 1) is configured to notify the security gateway of the alarm condition through the first network substantially simultaneously with notifying the monitoring station of the alarm condition through the second network (col. 1, lines 5-13)).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Powel (US 7,126,473) discloses intrusion detection and secure remote alarm communication system for a security system for the inactive storage of the active ingredients of weapons of mass destruction.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tung Vo whose telephone number is 571-272-7340. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Mehrdad Dastouri can be reached on 571-272-7418. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tung Vo/
Primary Examiner, Art Unit 2621